

How globalization is rapidly spurring financial services firms to raise the bar in information security and privacy*

The Global State of Information Security 2007

44%

Percentage of financial services respondents who said their company has mechanisms in place to report security incidents out to customers or business partners.

43%

Percentage of financial services respondents who report that their organization does not link security, either through organizational structure or policy, to privacy and/or regulatory compliance.

59%

Percentage of financial services respondents who say their company's information security policies do not include classifying the business value of data.

50%

Percentage of financial services respondents who report their organization performs an enterprise risk assessment either annually or semi-annually.

New opportunities often change benchmarking thresholds for core capabilities. And so it is in the financial services industry—which many believe has been defining best practices in protecting privacy and securing information for years. As global initiatives open doors to new channels for enhanced performance and shareholder value, many financial services firms are also assuming greater risks. Globalization is making it harder to centrally control and manage processes, policies and risks. And the web of collaborative arrangements continues to widen. As a result, it's getting harder to safeguard the sensitive information that supports building stronger relationships in a global marketplace. With increasing frequency, highly publicized data security breaches and concerns about identity theft are threatening to undermine trust, a cornerstone of the industry.

So this year we were pleased that 71% of the financial services respondents to the Global State of Information Security 2007—the world's largest survey on privacy and information security practices—now say their organization has a security strategy in place. This is a watershed gain over last year's reported level (57%). But keeping up with a shifting set of risks, opportunities and regulatory requirements globally will require expanding capabilities in several crucial areas.

- **As the global regulatory environment becomes more complex, gains in protecting data privacy have slowed.** Progress has flattened out in key areas as privacy governance issues continue to challenge executives. Financial services firms may be more likely this year to employ a Chief Privacy Officer (33% vs. 25% last year) and require employees to certify in writing that they are complying with privacy policies (65% vs. 56%) but firms are less likely to review their privacy policies annually (56% vs. 61%) and provide employees with privacy-related training (58% vs. 69%).
- **The “insider threat” may actually be growing.** Industry respondents reporting that employees represented the most probable source of security incidents increased significantly—from 34% in 2006 to 51%—a ranking that places employees ahead of hackers for the first time in this survey. Has the “insider threat” truly increased—or are companies simply more aware of the threat? It isn't clear. But 38% of financial services respondents identified the primary method of security incidents as either the abuse of valid user accounts and permissions or “social engineering”. In spite of this, few respondents say their organization has tiered authentication levels based on user risk classification (38%) or an automated account deprovisioning capability (27%).

Survey Methodology

The State of Information Security 2007, a worldwide security survey by PricewaterhouseCoopers and CIO Magazine, was conducted online from March 6 to May 4, 2007. Readers of CIO Magazine and clients of PricewaterhouseCoopers from around the globe were invited via email to take the survey. The results discussed in this report are based on the responses of 7,200 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries. The margin of error is $\pm 1\%$.

This year, there were 1,193 respondents (17% of survey) from the financial services sectors (commercial banking, consumer banking, property and casualty insurance, investment management, mortgage banking, capital markets and real estate). Of these, 46% were from North America, 25% from Europe, 20% from Asia, and 8% from South America. One-third (40%) reported annual revenues of at least \$1 billion.

To learn more about the survey, or about how PwC helps companies address security and privacy issues, visit: www.pwc.com/giss2007 or contact:

Mark Lobel
646 471 5731
mark.a.lobel@us.pwc.com

Kurt Gilman
646 471 8830
kurt.gilman@us.pwc.com

John Garvey
646 471 2422
john.garvey@us.pwc.com

- **Dedicating more resources to protecting data is becoming an increasingly strategic priority.** Most financial services respondents (58%) say their organization does not maintain an accurate inventory of user data and only 37% keep an inventory of all third parties using customer data. The survey also indicates that the number of incidents resulting in compromise to customer records jumped from 19% in 2006 to 26% this year. Financial services organizations aren't much better than the cross-industry average at encrypting data in databases (51% vs. 50%), file shares (35% vs. 36%) and backup tapes (44% vs. 38%). Only about half (54%) report deploying laptop encryption—a key data security safeguard for an increasingly mobile workforce at a time when lost or stolen unencrypted laptops can trigger notification requirements.
- **Measurement and monitoring: Rules are only effective if they're followed.** A crucial area where financial services firms have made significant progress is in defining the policies they expect to be carried out across expanding global enterprises. This year, a significantly greater percentage of financial services respondents report their security policies now address the collection of security metrics (40% vs. 29%) as well as enforcement mechanisms or standards (46% vs. 36%). What gives us pause, however, is that only 6 out of 10 industry respondents say their company has measured and reviewed the effectiveness of its information security policies and procedures within the past year.
- **Outsourcing processes to third parties doesn't transfer risk—it often increases it.** One of the often overlooked aspects of compliance—and of sourcing, for that matter—is that ultimate responsibility for protecting sensitive information rarely can be passed on to third-party vendors. Financial services regulators are increasingly focused on vendors' privacy and data-handling practices and any resulting risks to the confidentiality of customer data. So as financial services organizations expand their global footprints, the fact that 70% of their survey respondents are only "somewhat" or "not at all" confident in third-party security raises red flags. Just over half (56%) require third parties (including outsource vendors) to comply with the organization's own privacy policies and only 56% have established security baselines for external partners, customers and suppliers.

Security benchmarks: Financial Services

(Percentage of responses from Financial Services vs. other industries)

	FS 2007	FS 2006	All 2007
Have an overall security strategy	71%	57%	57%
Have an identity management solution	33%	31%	28%
Have a centralized security information management process	57%	51%	44%
Deploy security event correlation technologies	38%	20%	29%
Have security procedures for handheld/portable devices	44%	40%	32%

© 2007 PricewaterhouseCoopers LLP. All rights reserved. "PricewaterhouseCoopers" refers to PricewaterhouseCoopers LLP (a Delaware limited liability partnership) or, as the context requires, the PricewaterhouseCoopers global network or other member firms of the network, each of which is a separate and independent legal entity. SJ-08-0018-A 08-07 DB



Business
Technology
Leadership

